University of Kent

Addressing Cybersecurity and Cybercrime via a co-Evolutionary aPproach to reducing human-relaTed risks: Healthcare as a use case

Shujun LI (李树钧)

Professor of Cyber Security, School of Computing

Director, Kent Interdisciplinary Research Centre in Cyber Security (KirCCS)

http://www.hooklee.com/

@hooklee75

Human-Related Risks: The GDPR Context

DPIA required!

- A **Data Protection Impact Assessment (DPIA)** is required by the EU GDPR 2016 when
  - **High risk** to rights and freedoms of data subjects
  - Systematic and extensive evaluation of **personal aspects relating to natural persons** (e.g., automated processing, profiling, decisions producing legal effects)
  - **Large scale** processing of **sensitive** (e.g., **genetic and biometric**) or **crime** related data
  - **Surveillance** ("*a systematic monitoring of a publicly accessible area on a large scale*")
- As we all know, GDPR will come in force from **25th May 2018** in the whole EU (including the UK!).

What in a DPIA?

- It shall contain (Article 35(7) of GDPR)
  a) a **systematic** description of the envisaged **processing operations** and the **purposes** of the processing, including, where applicable, the **legitimate interest** pursued by the controller;
  b) an assessment of the **necessity** and **proportionality** of the processing operations in relation to the purposes;
  c) an assessment of the **risks** to the rights and freedoms of data subjects; and
  d) the **measures** envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
- + **Prior consultation** (“where appropriate”) (Article 36 of GDPR)

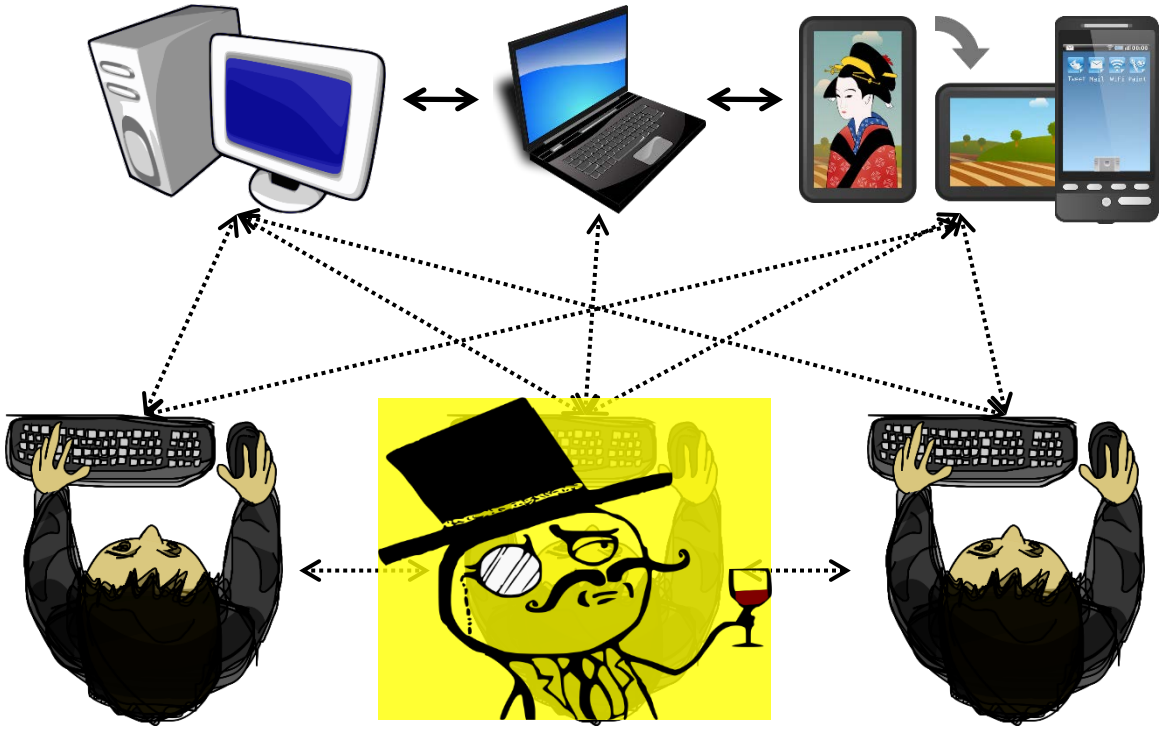
What risks?

- Risks to individuals
  - Rights (right to life, privacy as a human right, …)
  - Freedom
- Consequent risks to the organisation
  - Legal (non-compliance)
    - Regulatory action
  - Financial loss
    - Legal costs
    - Compensation to affected people and organisations
    - Reduced revenue
  - Reputation / Public trust

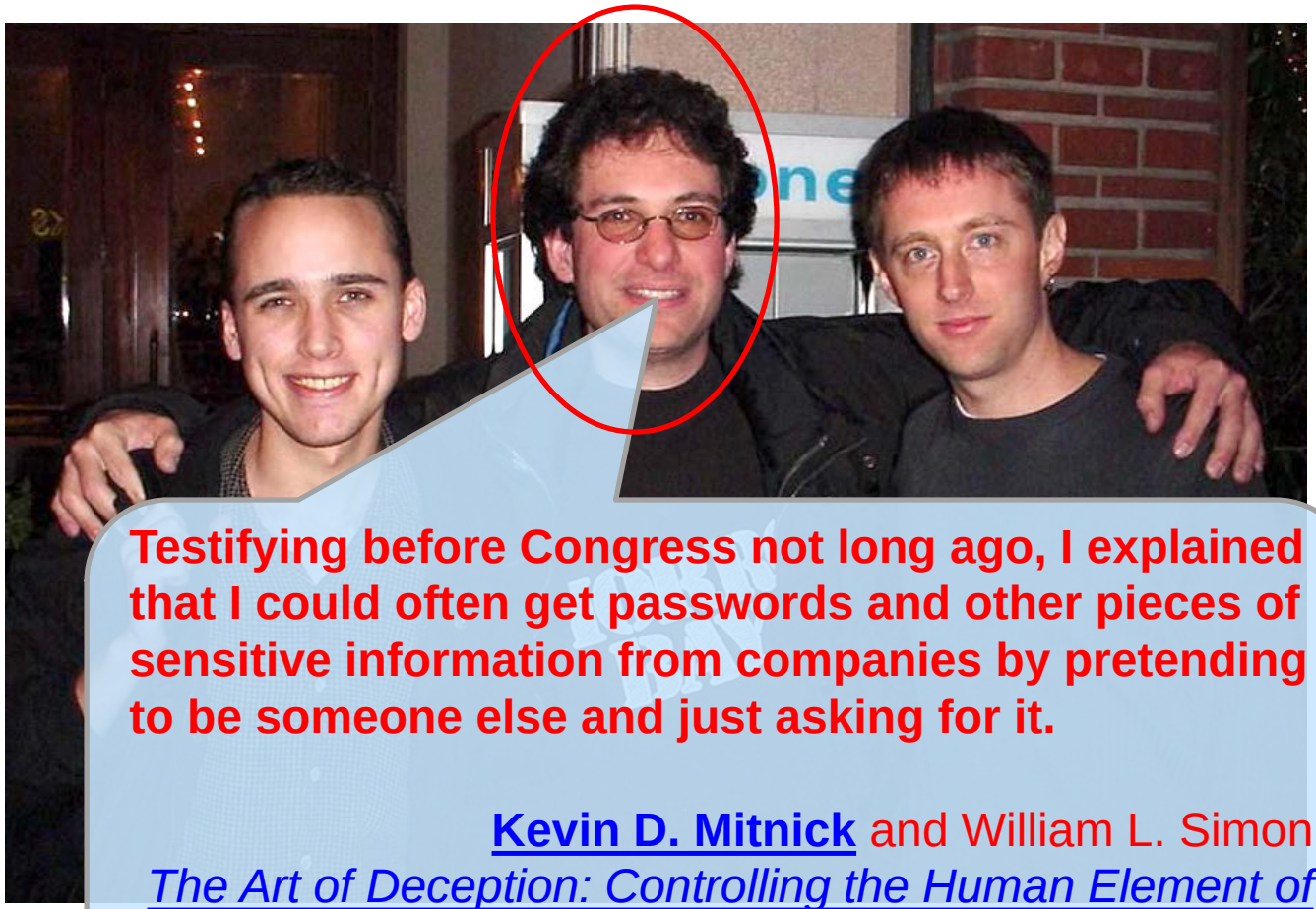
Human-Related Risks

Social engineering

- Hackers only need to break the weakest link in a security process/system – humans!
- Weak human users vs. Strong hackers

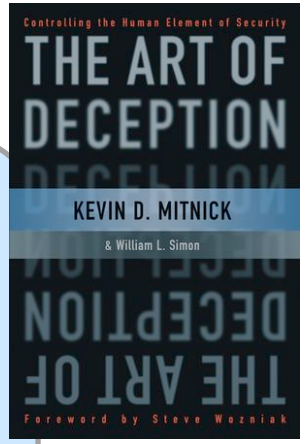


A real hacker said…



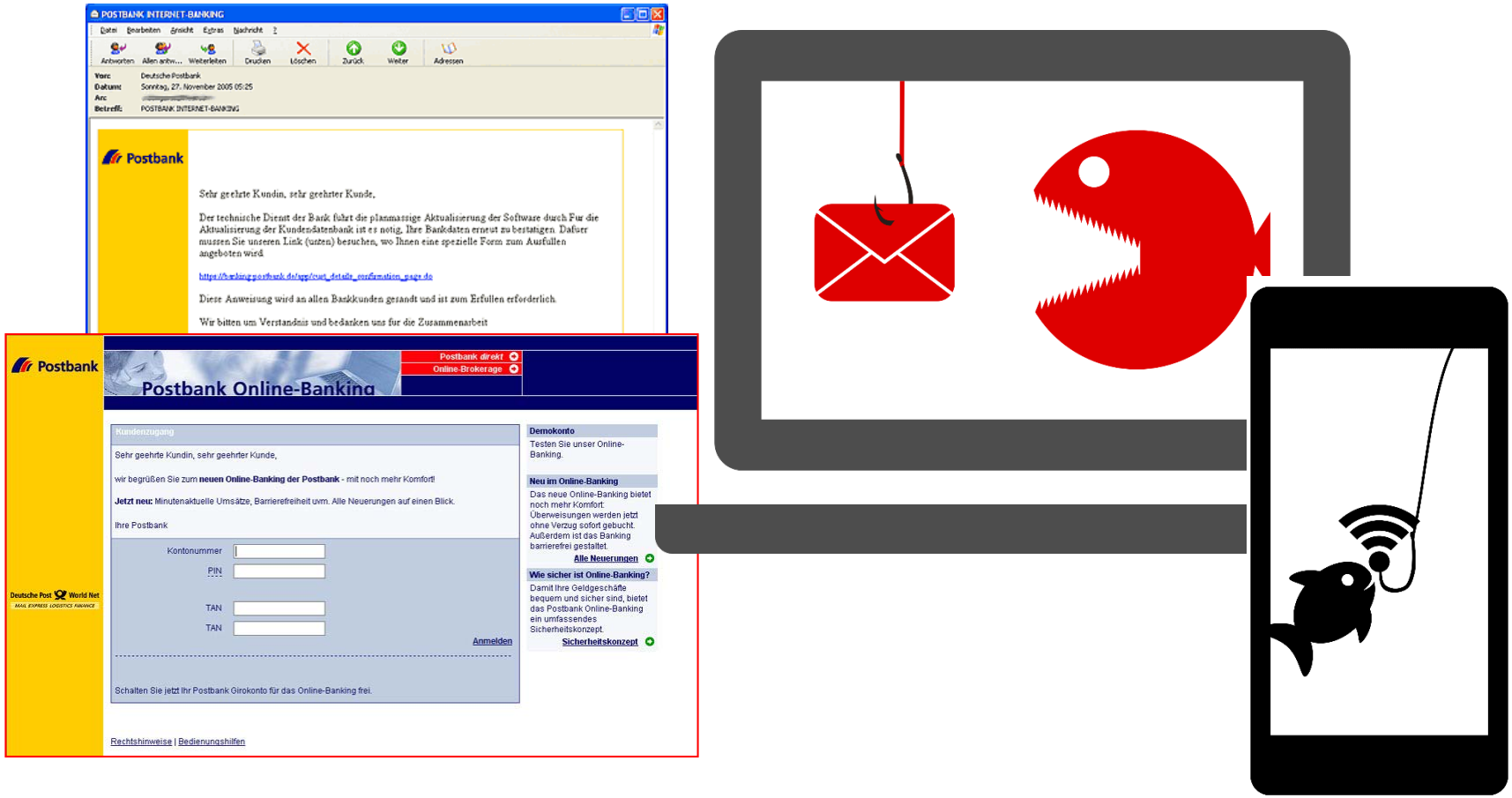
Testifying before Congress not long ago, I explained that I could often get passwords and other pieces of sensitive information from companies by pretending to be someone else and just asking for it.

Kevin D. Mitnick and William L. Simon
The Art of Deception: Controlling the Human Element of Security, John Wiley & Sons Inc., 2003



Phishing…

- Getting your password (and data) from you.



Weak humans everywhere!

- Weak designers
- Weak programmers
- Weak assemblers
- Weak distributors
- Weak deployers
- Weak maintainers
- **Weak users**
- Weak …

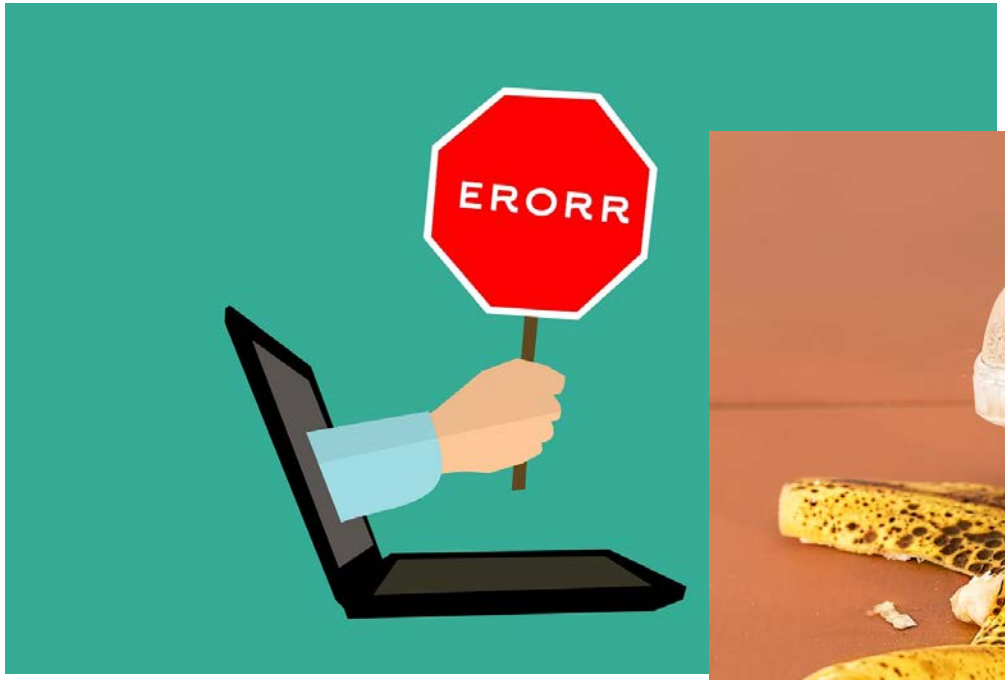
⇒ Security holes in the delivered products

Strong Hackers

⇒ Security holes in the deployed system

And don’t forget about human errors!

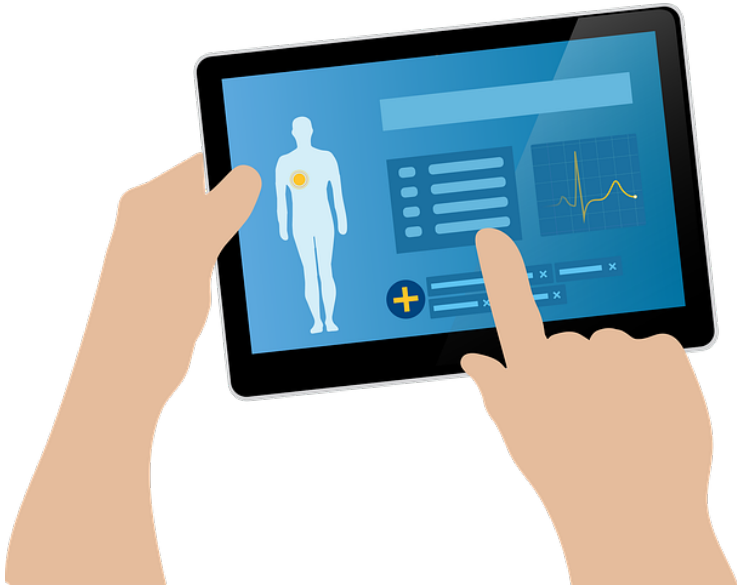
- As humans, we make errors all the time, often unintentionally.



Human-Related Risks:
Some Scenarios in Healthcare

DPIA in hospitals and GP clinics

- Weak passwords and improper password policies
- Bring your own devices (BYOD)
- Software patching (policies and operation)
- Phishing emails
- Rogue WiFi access points
- Insecure websites
- Shoulder surfers
- Malicious insiders
- Human errors
- …



IoT-based home care

- Potential risks
  - Data breaches (at home, on the way, and at the home care provider's end)
  - Manipulated data (can lead to death of patient)
  - Privacy violations
  - …
- Privacy of
  - Patient(s)
  - Carer(s)
  - Family members who are not carers or patients but living in the same household
  - Visitors / Neighbours / …

University of Kent

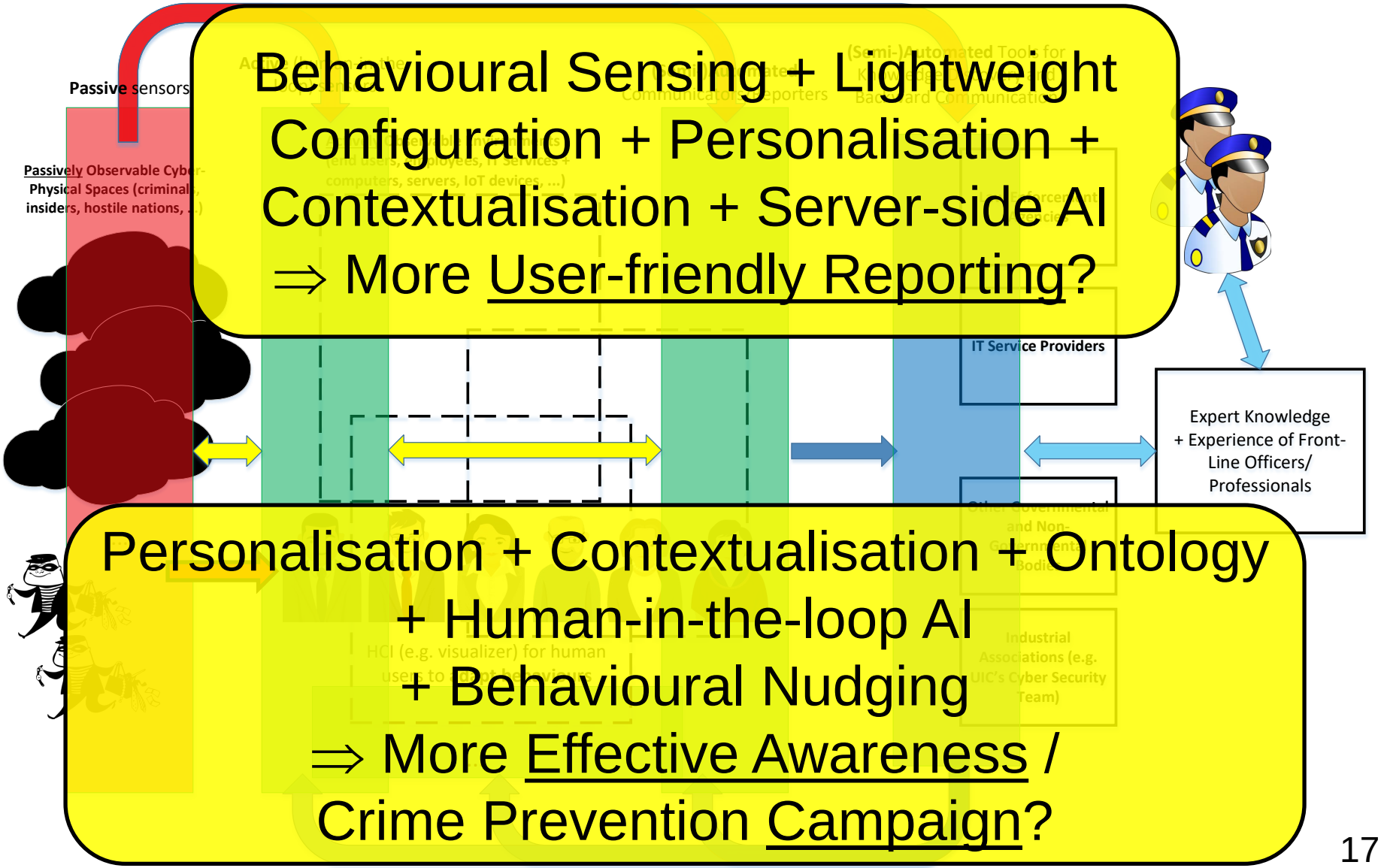
The Project ACCEPT: Addressing Cybersecurity and Cybercrime via a co-Evolutionary aPproach to reducing human-relaTed risks

EPSRC
Engineering and Physical Sciences Research Council

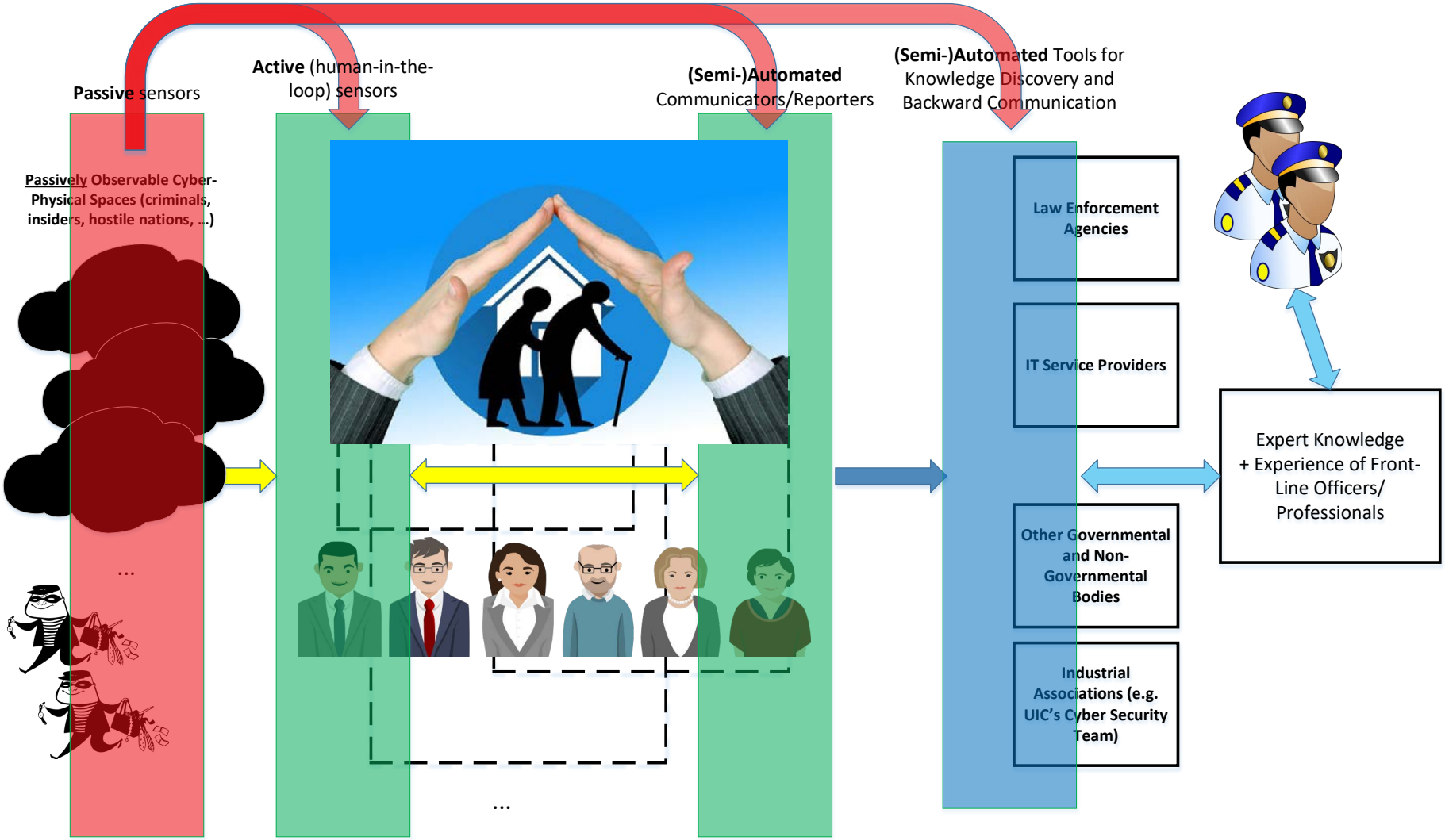
Overall aim

- To reduce human-related risks via developing a **socio-technical framework and corresponding software tools** through which we can
  a) analyse the behavioural co-evolution of cybersecurity/cybercrime ecosystems
  b) effectively influence behaviours of a range of actors in the ecosystems
     ⇒ Reducing human-related risks
     ⇒ Converting human from the weakest link to the strongest link!

Technical framework



Technical framework: Home care



Who are beneficiaries?

- Designers and developers of solutions
- Cyber security educators, trainers, awareness campaigners, etc.
- Law enforcement agencies
- **Citizens / Businesses / Employees**
  - **For healthcare**: Doctors, nurses, carers, patients, managers, staff of IT department, …
- …
- Users need **incentives** to cooperate!
  - They get personalised feedback and recommendations.
  - And more direct incentives?

Incentivising users (inc. organisations)

- Valuing users' contributions
- Offering credit to users who have contributed
- Offering more credit to users who have contributed more and been more actively
- Potential use of **cryptocurrency**

  - User ⇒ Our Project (Trusted Centre) / Organisations / Communities: **Proof of Value (PoV)**
  - Our Project (Trusted Centre) / Organisations / Communities ⇒ Contributing Users: tokens / coins
  - A **consortium blockchain** is likely what we need.
  - Personal data should be **anonymised** to avoid unnecessary risks.

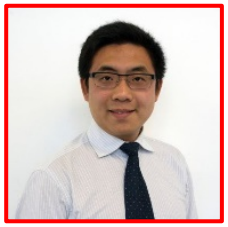
The highly-interdisciplinary team












1. Computer Science
2. Crime Science
3. Business
4. Engineering
5. Behavioural Science

Use cases being considered

- Cyber Fraud
  - Human-related risks to **cyber** fraud
- Finance
  - Human-related risks to **cyber** attacks within global financial transaction and exchange networks
- Transport
  - Human-related **cyber(-physical)** risks to privacy attacks and other attacks within hybrid transportation networks
- **Healthcare**
  - Human-related **cyber(-physical)** risks to safety and privacy attacks in healthcare applications

How to collaborate?

- Expert opinions
- Crime cases (not limited to cyber crime)
- Cyber security incidents
- Statistical data
- Access to relevant people (cyber criminals, victims and their families, etc.)
- Participation of interviews, surveys, focus groups, workshops, lab-based user studies
- Helping to run field studies in real world
- Helping to disseminate our results
- …

Stakeholders Group

- Public sector organisations
  - Europe: European Cybercrime Centre (EC3), Europol
  - UK (national): Metropolitan Police Services (MPS), British Transport Police (BTP)
  - UK (regional): Southeast Regional Organised Crime Unit (SEROCU), Surrey & Sussex Police
  - Others: Highways England
- Industry
  - Cyber security: IBM UK, BAE Systems Applied Intelligence, NCC Group, Crossword Cybersecurity plc
  - Financial sector: Lloyds Banking Group
  - Transport: UIC – International Union of Railways
- Not-for-profit organisations
  - Neighbourhood and Home Watch Network, HAT Community Foundation (HCF)

We are keen to engage wider stakeholders as well!

A take-home message

University of Kent

Security that doesn't work for people doesn't work.

Thanks for your attention!

Questions?

Methodology

- Theories
  - Criminology, evolution (biology), behavioural economics, business, …
- ⇓
- Computational ontology
- Knowledge base
- ⇑
- Crime cases and security incidents
- Data from interviews, focus groups, surveys, lab-based studies and software tools, …

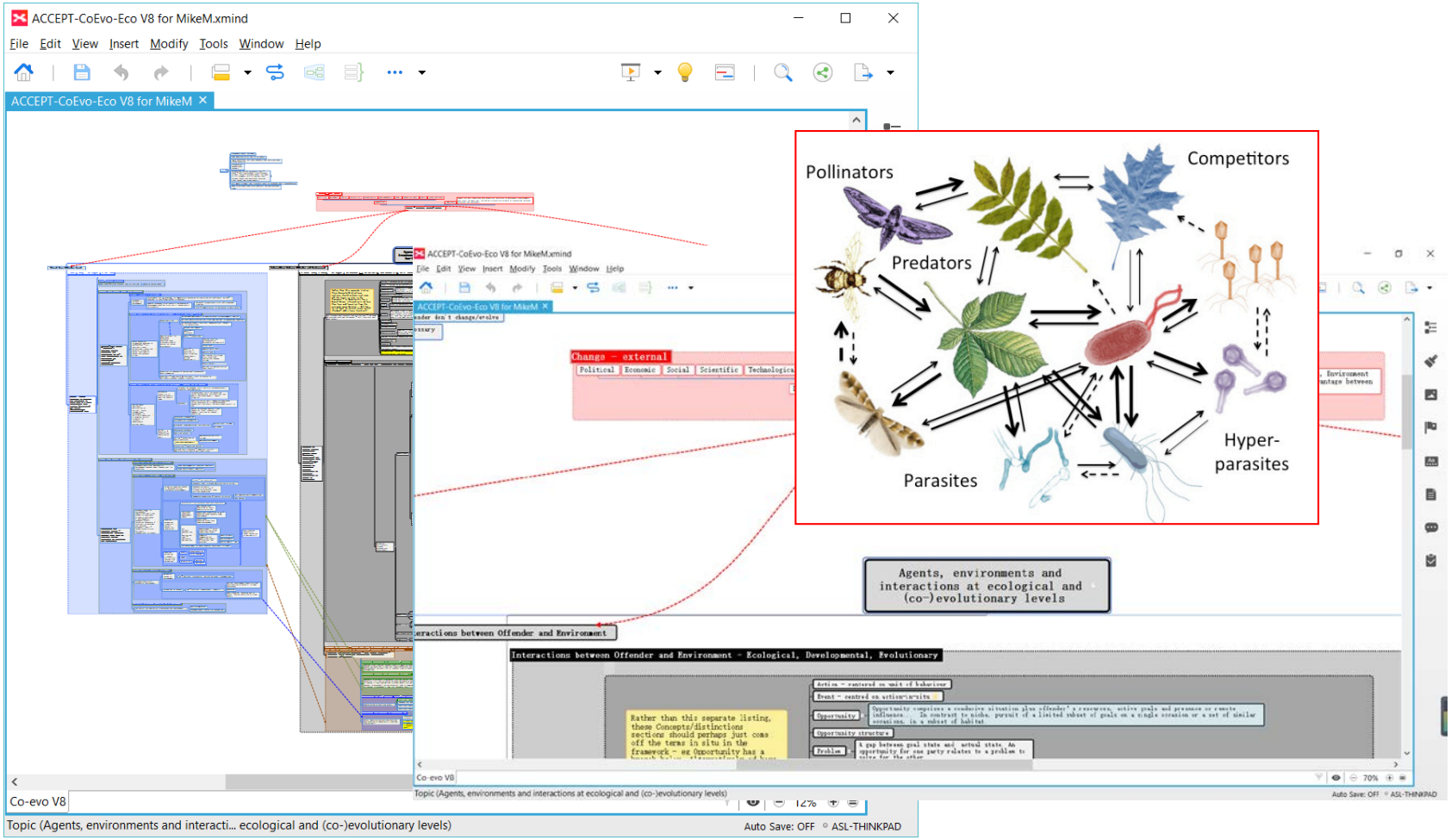
⇒ **Co-Evolutionary Socio-Technical Framework**

Top-down

Bottom-up

Ontology

- Computational cyber crime/security ontology



Advisory Board

Chair